UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	17-cr-64-DWF-KMM
	)	
v.	)	**MEMORANDUM IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS**
	)	
EDWARD S. ADAMS,	)	
	)	
Defendant.	)	

INTRODUCTION

The government violated the Fourth Amendment and invaded the attorney-client and marital privileges when it obtained from Yahoo! (via a search warrant) more than 100,000 emails sent to or from two email addresses (including the principal one) of Mr. Adams, a practicing attorney. The government worded its warrant application to convey the clear impression that, upon obtaining the electronically stored information ("ESI") from Yahoo!, it would set up a process by which certain persons would search for and identify emails relevant to certain subjects, so that the prosecution team would not review privileged or irrelevant emails. In fact, however, the prosecution team had free access to thousands of emails having nothing to do with any of the subjects listed in the warrant—including numerous privileged emails.

What was said of a government request for a warrant encompassing all emails associated with various email accounts is equally apt here:

> [T]he breadth of the information sought by the government's search warrant for the target accounts—including the content of every email sent to or from the accounts—is best analogized to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. ***The Fourth Amendment would not allow such a warrant and should therefore not permit a similarly overly broad warrant just because the information sought is in electronic form rather than on paper***.

In re Applics. for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO, 2013 WL 4647554, at *8 (D. Kan. Aug. 27, 2013).[1] "[E]mail requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve." *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010).

The way the government proceeded here was especially objectionable both (i) because the government did not take reasonable steps to separate out emails unrelated to the subjects listed in the warrant and (ii) because, before the government sought the warrant, it was on notice that many of the emails Mr. Adams sent or received likely would be privileged. As the government knew but did not disclose to Magistrate Judge Rau, who approved the warrant that ultimately was executed, Mr. Adams was represented by counsel in a then-ongoing SEC investigation and had been represented by counsel in four civil suits relating to the matters at issue here. The government's criminal

[1] Unless otherwise indicated, all emphasis in quotations has been added by counsel.

investigation involved the same transactions and conduct that had been the subject of the SEC investigation and the civil suits.

The government's violation of the Fourth Amendment and the attorney-client privilege did not stop when it served the warrant on Yahoo!. Upon obtaining Mr. Adams's emails, certain (unidentified) government agents purportedly divided them into two groups, one containing emails that allegedly were non-privileged and related to the subjects listed in the warrant, and one containing the remaining emails. The prosecution team purportedly had access only to the former group. But the government has repeatedly refused to disclose the steps it took to divide the emails, and whatever steps it took were completely inadequate. Indeed, the government's methods left numerous privileged communications among the emails to which the government has admitted the prosecution team was given access. In addition, there can be no assurance that all information about the nearly 80,000 emails the government categorized as potentially privileged or unrelated to the subjects listed in the warrant was withheld from the prosecution team.

This Court should suppress the emails seized from Yahoo! and all evidence derived therefrom, both because the search warrant amounted to an unconstitutional general warrant and because the warrant was executed in an unreasonable manner. The government should be directed to destroy or return all of the information obtained from Mr. Adams's Yahoo! accounts. Alternatively, an evidentiary hearing should be held to develop a full record concerning the government's handling of the emails.

BACKGROUND

A. The Companies Involved.

This case principally concerns four companies.

The first, Apollo Diamond, Inc. ("Apollo Diamond"), was founded by Robert Linares, Mr. Adams's father-in-law, who is referred to in the Indictment as "Apollo Employee A." Indictment ¶ 7.

The second, Apollo Diamond Gemstone Corp. ("Apollo Gemstone"), was a subsidiary of Apollo Diamond. (Apollo Diamond and Apollo Gemstone are collectively referred to herein as "Apollo"). *Id.* ¶ 3.

The third company, referred to in the Indictment as "Private Scio," was a privately-held company created in 2011 in order to purchase the assets of Apollo. *Id.* ¶¶ 43–44. Apollo shareholders were able to sell back their Apollo shares for a penny per share, and purchase the same number of shares of Private Scio, also for a penny per share. *Id.* ¶ 45.

After shareholders approved Private Scio's purchase of substantially all of the assets of Apollo, a fourth company, Scio Diamond Technology Corporation ("Public Scio") exercised the rights it had been assigned by Private Scio to acquire Apollo's assets. *Id.* ¶¶ 48, 56. Public Scio is a publicly-traded company. *Id.* ¶ 52.

B. Mr. Adams.

Edward S. Adams resides with his wife, Denise Adams, and their fourteen-year-old son in Minneapolis. He was at all pertinent times and still is the Howard E. Buhse Professor of Law and Finance at the University of Minnesota Law School.

For most of the time period at issue in this case, Mr. Adams was also a partner in the Minneapolis law firm of Adams Monahan LLP (originally Adams, Monahan & Sankovitz) and served as General Counsel of Apollo Diamond. *Id.* ¶¶ 4–5. Adams Monahan provided legal services to Apollo. *Id.* ¶ 14. In addition to serving as General Counsel of Apollo Diamond, at various times Mr. Adams held other positions at Apollo Diamond and Apollo Gemstone. *Id.* ¶ 4. As a partner at Adams Monahan, Mr. Adams represented numerous clients unaffiliated with Apollo in connection with a variety of corporate, bankruptcy, and intellectual property matters. Mr. Adams also was retained by other attorneys as a consultant or expert witness.

Well before the government applied for a search warrant as part of its criminal investigation, Mr. Adams became the subject of an SEC investigation, *In re Scio Diamond Technology Corporation* (C-08091), that concerned the acquisition of the assets of Apollo Diamond and the exchange of shares in Apollo Diamond for shares in Private Scio. As the government was well aware when it served the warrant on Yahoo! in this matter, Mr. Adams was represented in the SEC investigation by attorneys James Farrell and John J. Sikora, Jr. of Latham & Watkins LLP ("Latham") and attorney James L. Kopecky of the Chicago law firm of Kopecky Schumacher Bleakley & Rosenburg, P.C. *See* Decl. of Lance A. Wade ¶ 6 & Ex. 5 at 2. Mr. Adams was deposed at length by SEC attorneys on August 27, 2015 and October 8, 2015, and the United States Attorney's Office in Minnesota ("USAO") obtained transcripts of those depositions. *Id.* ¶ 7. In February of this year, the SEC notified Mr. Adams that it had decided not to pursue an enforcement action against him in connection with its investigation. *Id.* ¶ 8.

After the USAO opened a criminal investigation relating to these same matters, Mr. Adams was represented in that investigation by Jon M. Hopeman, then of Felhaber Larson. *Id.* ¶ 9. The USAO was aware by at least mid-February 2016 that Mr. Adams was obtaining counsel to represent him in the USAO's investigation, and was introduced to Mr. Hopeman specifically by early March 2016. *Id.*

Mr. Adams also was represented by counsel in four civil suits relating to the Apollo companies that were brought by disgruntled shareholders of Apollo Diamond, Private Scio, and/or Public Scio in 2012 and 2013. *Id.* ¶ 10. As reflected in publicly available filings and dockets, and as may also have been known to the government from its contacts with those shareholders, Mr. Adams was represented in two of the suits by attorneys from Latham and an attorney at the Charleston, South Carolina law firm of Moore & Van Allen PLLC, in a third suit by attorneys from Latham, and in a fourth suit by Aaron R. Hartman of Monroe Moxness Berg P.A. *Id.* ¶¶ 10-12 & Exs. 6-9. One of the suits was the subject of questioning by the SEC when it deposed Mr. Adams in 2015. *Id.* ¶ 12 & Ex. 5 at 451-55.

At his deposition before the SEC on August 27, 2015, Mr. Adams testified that the email address that he had mainly used was edwardsadams@yahoo.com. *Id.* ¶ 13 & Ex. 5 at 12. He also explained that he sometimes used the email address jafman1@yahoo.com, including for matters relating to Apollo. *Id.* ¶ 13 & Ex. 5 at 368.

C. The Government's Application for the First Search Warrant.

When the government first applied for a search warrant in late 2015, it knew of many of Mr. Adams's attorney-client relationships and the likelihood that data stored in

his Yahoo! email accounts would contain attorney-client communications. At that time, the government knew that (a) Mr. Adams was a practicing attorney and a law professor; (b) edwardsadams@yahoo.com was his primary email account; (c) he was represented by counsel in the then-ongoing SEC investigation and had been represented by counsel in the related civil suits; (d) he had served as Apollo Diamond's General Counsel for many years; and (e) he had represented clients as a partner at Adams Monahan. Nevertheless, the government set out to seize without restriction *all* emails in Yahoo!'s possession that were ever sent to or from edwardsadams@yahoo.com or jafman1@yahoo.com.

In November 2015, Postal Inspector Christie Kroells of the U.S. Postal Inspection Service applied to Magistrate Judge Mayeron for a warrant to seize from Yahoo! any information associated with three email addresses: edwardsadams@yahoo.com, jafman1@yahoo.com, and michaelrmonahan@yahoo.com, an email account belonging to Michael Monahan, Adams's law partner at Adams Monahan. Ex. 1 at 1.

Inspector Kroells told Magistrate Judge Mayeron that "[b]etween 2004 and 2011, Adams held various positions within both [Apollo Diamond] and [Apollo Gemstone], including Secretary of [Apollo Diamond] and Secretary, Executive Vice President, Chief Financial Officer, Director, and President of [Apollo Gemstone]" and had "reviewed records showing Adams in these roles." *Id.* at 5 (¶ 8). Inspector Kroells also stated that Michael Monahan had been the General Counsel of Apollo Gemstone, among other positions he held with that company. *Id.* (¶ 9). But she did *not* inform Magistrate Judge Mayeron that Mr. Adams had served as General Counsel of Apollo Diamond, even though the government plainly knew that fact, at a minimum because it was disclosed by

Mr. Adams in his August 27, 2015 deposition before the SEC (of which Inspector Kroells had a transcript when she prepared her affidavit). *Id.* (¶¶ 14, 33); Wade Decl. ¶ 7 & Ex. 5 at 64.

The warrant application also failed to disclose that Mr. Adams was represented by counsel in the then-active SEC investigation. And it gave no indication that he had been a defendant in multiple civil suits involving allegations overlapping with the subject of the criminal investigation, let alone that he was represented by counsel in each of those suits.

With respect to the disclosure of ESI by Yahoo!, the warrant contained no limitation as to either time period or subject matter. Section I of Attachment B to the warrant stated that, for each of three listed email accounts, Yahoo! was to disclose to the government, *inter alia*, "[t]he contents of *all e-mails* associated with the account, including stored or preserved copies of e-mails sent to and from the account, [and] draft e-mails . . . ." Ex. 1 at 24.

The warrant, however, plainly implied that the government would search the ESI disclosed by Yahoo! and "seize[]" only ESI pertaining to three subjects. Section II of Attachment B was entitled "Information to be *seized by the government*" and read as follows:

> a. All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 United States Code, Sections 1341 and 1343, those violations involving Edward S. Adams and Michael R. Monahan and occurring after October 25, 2006, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. All documents, records, and communications related to financial, bookkeeping, transactional, and tax records reporting the business and financial transactions of ADI, ADGC, Private Scio, Public Scio, Focus, and ESA during and for the calendar, fiscal, and federal tax years 2010 to present; to include, but not limited to:
    i. All bookkeeping ledgers, journals, reports, and other bookkeeping records, and computer printouts thereof, which itemize and record the dates, amounts, purpose, and expense category and classification of all financial transactions conducted in and through the business bank accounts and other financial accounts of the above business entities.
    ii. All bookkeeping ledgers, journals, reports, and other bookkeeping records, and computer printouts thereof, which record, identify, and itemize the dates, amounts, and nature and classification of all income and expenses of the above business entities.
2. All documents, records, and communications related to Private Scio, Public Scio, to include all such documents, records, and communications regarding the ADI/ ADGC proxy statement from March 2011, the asset purchase agreement between ADI/AGC and Private Scio, the stock-repurchase program, and the private offering.
3. All documents and records reflecting communications with shareholders or prospective shareholders of ADI, ADGC, Private Scio, and Public Scio.

Id. at 25–26.

The requested warrant was issued by Magistrate Judge Mayeron, with a "SEARCH WARRANT ADDENDUM" attached. *Id.* at 1, 28. The Addendum stated that "the government shall establish a search methodology . . . to ensure that no attorney-client privileged communications will be inadvertently reviewed by the prosecution team." *Id.* at 28. It further stated that, if material seized pursuant to the warrant were

> identified by the government as possibly containing attorney-client privileged communications, an Assistant United States Attorney, who is not a member of the prosecution team and who is not participating in the search, shall act as a "taint team" to set up an ethical wall between the evidence and the prosecution team that will prevent any privileged material from getting through to the prosecution team.

Id.

Inspector Kroells then faxed the warrant to Yahoo!. Ex. 3 at 21 (¶ 41). Yahoo!, however, informed the government that the company no longer accepted service of warrants by fax. *Id.*; *see also* Ex. 2 at 2.

D. The Government's Application for the Second Search Warrant.

Its service of the first warrant having failed, the government applied for a second warrant in January 2016, on this occasion to Magistrate Judge Rau. Ex. 3 at 1. It again sought disclosure by Yahoo! of any information associated with the three email accounts, including all emails and draft emails regardless of time or subject matter. This time, the government was even less forthcoming than it had been the first time.

In the second application, Inspector Kroells again stated that Mr. Adams had held various positions at Apollo. *Id.* at 4 (¶ 8). But once again, she omitted any mention of Mr. Adams's role as General Counsel of Apollo Diamond. *Id.* And again she did not disclose his representation by counsel in the SEC investigation or in the four private civil suits. *Id.*

Inspector Kroells did modify her warrant application to note that Magistrate Judge Mayeron had issued a search warrant pertaining to the same three email addresses, and that the earlier warrant "was based on the same allegations contained in this affidavit."

Id. at 21 (¶ 41). But she did *not* inform Magistrate Judge Rau that the warrant signed by Magistrate Judge Mayeron had contained a "SEARCH WARRANT ADDENDUM" identifying procedures to prevent access by the prosecution team to privileged communications. The warrant proposed to Magistrate Judge Rau identified no such procedures.

As with the first application, Inspector Kroells drew a distinction in the proposed warrant between the ESI to be disclosed by Yahoo! and the ESI to be "[s]eized" by the government, implying that ESI not related to the subjects listed would be culled out after the government received the ESI. *Id.* at 24–26 (Attachments I & II). Magistrate Judge Rau issued the requested warrant. *Id.* at 1.

E. The Government's Handling of the ESI Disclosed by Yahoo!

After the government served the second warrant on Yahoo!, the company responded by producing more than 400,000 pages of ESI associated with the three email addresses. Wade Decl. ¶¶ 14, 20 & Ex. 4. Yahoo! disclosed 108,291 emails or draft emails from Mr. Adams's accounts: more than 70,000 associated with edwardsadams@yahoo.com and nearly 38,000 associated with jafman1@yahoo.com. *Id.* ¶ 20. Yahoo! also disclosed emails from Mr. Monahan's Yahoo! account. *Id.* The emails date back to October 2006. *Id.*

In May 2017, the government produced to the defense, pursuant to its Rule 16 obligations, a hard drive containing ESI that had been produced to it by Yahoo! from the three email accounts. *Id.* ¶ 15 & Ex. 10. The government purported to provide two databases, one (which it called "Yahoo email unfiltered") supposedly containing all of

the emails produced by Yahoo! and one (which it called "Yahoo email filtered") supposedly containing "potentially privileged, as well as non-responsive, emails and documents" from the Yahoo! production. *Id.* ¶ 16 & Ex. 10.

But the government's account of what the two databases contained was inaccurate. This became apparent when defense counsel reviewed the ESI the government produced, and defense counsel immediately informed the government of the discrepancy. Wade Decl. ¶ 17 & Ex. 11 at 6. On June 5, 2017, the government responded by conceding that its earlier statements about the hard drive had been erroneous:

> I checked on this with our lit support folks, and, apparently, they did not understand what our paralegal had requested. On the hard drive that you received, they did not include the full set of data for the two Adams accounts (edwardsadams@yahoo.com and jafman1@yahoo.com) that we received from Yahoo.

Id. ¶ 18 & Ex. 11 at 3-4. The government stated that it would separately supply the complete data received from Yahoo!. More importantly, however, the government acknowledged that the prosecution team had been given access to "the folder that was labeled 'Adams_Yahoo_Unfiltered' on the drive that [the defense] received." *Id.* ¶ 18.

1. The 108,291 Files from Mr. Adams's Yahoo! Email Accounts

Among the emails obtained by the government is information of the highest order of sensitivity to an individual under criminal investigation: privileged communications between Mr. Adams and his counsel regarding his recollections and understandings of the facts, as well as legal strategy and applicable defenses, in the very criminal investigation in which the warrant was obtained. Privileged communications with his attorneys in the SEC investigation and prior civil suits also were disclosed by Yahoo! and raise similar

concerns given their relatedness to the subjects of the criminal investigation. *See id.* ¶ 21. Even according to the government, which failed to identify or treat as privileged many emails that demonstrably are privileged, the vast majority of the email files obtained from Yahoo!—more than 70%—are potentially privileged or irrelevant to the subjects listed in the warrant. *Id.* ¶ 22.

The government isolated more than 79,000 such files into a separate database, using methods the government has refused to disclose to Mr. Adams or his counsel.[2] *Id.* ¶ 32. The Assistant U.S. Attorneys prosecuting the case have represented that *they* have had no access to that isolated set of emails, but the extent of other governmental intrusion into those protected communications remains undisclosed and unknown. This database of privileged, irrelevant, and extraordinarily sensitive communications has been in the hands of government personnel for over twenty months and remains so today. *Id.* ¶ 34.

2. The 29,010 Files Provided to the Prosecution Team

Unidentified government personnel filtered out nearly two-thirds of the Yahoo!-produced files based on criteria that the government refuses to disclose to the defense. It then passed along to the prosecution team the remaining approximately 29,000 files that it appears to have concluded were not subject to any privileges and were properly called for in the warrant. *See* Wade Decl. ¶ 22. Yet, based on time-consuming searches and

[2] Although it would in no way represent an adequate remedy for the government's Fourth Amendment violations, the over 79,000 Yahoo! files the government has identified as privileged or irrelevant ought to be returned to Mr. Adams or destroyed immediately. *See* Section I *supra*.

reviews the defense has conducted to date, it appears that at least 5,000 of those files, and potentially as many as nearly 10,500 emails, are privileged. *Id.* ¶ 23. Hundreds of other emails are wholly unrelated to the subjects identified in the warrant. *Id.* Over 900 documents appear to implicate Mr. Adams's personal attorney-client privilege with his own counsel. *Id.* ¶ 24. By way of example, until just last month, the prosecution team had access to emails from July 2012 (many of which were marked "PRIVILEGED ATTORNEY CLIENT COMMUNICATION") among Mr. Adams, Mr. Monahan, and Aaron Hartman, an attorney then at Anthony Ostlund Baer & Louwagie P.A., about then-pending litigation with shareholders of Apollo, Private Scio, and Public Scio in which Mr. Hartman represented Mr. Adams and Mr. Monahan. *Id.* Over 1,600 other emails appear to involve Mr. Adams's communications with his own clients, regarding either his legal work for them or matters in which he had been retained as a consultant or expert witness. *Id.* ¶ 25. Additionally, more than 300 emails implicate the spousal privilege he shares with his wife. *Id.* ¶ 26. Unsurprisingly, in light of the fact that Mr. Adams's father-in-law and brother-in-law were active officers of Apollo—a circumstance known to the government at the time it seized Mr. Adams's Yahoo! emails—dozens of the private spousal communications to which the prosecution team has had access relate to Apollo. *Id.*

Also among the documents provided to the prosecution team are more than 200 emails entirely unrelated to the subjects of the Indictment, including, for example: more than one hundred emails about the planning of a surprise 50th birthday party for Mr. Adams's wife (including drafts of a poem Mr. Adams wrote to her for that occasion);

more than sixty emails relating to a yogurt business owned by Mr. Adams; emails about ski trips taken by Mr. Adams; travel itineraries for family vacations; emails concerning a potential personal investment by Mr. Adams in a Chicago hotel; and emails relating to evaluations of coaches of children's sports teams in which Mr. Adams was involved. *Id.* ¶ 27.

Many of these emails in the folder made available to the prosecution team bear familiar labels—applied contemporaneously by the senders—signaling the presence of privileged communications or work product materials. *Id.* ¶¶ 28-29. Others were sent to or from attorneys for Mr. Adams whose names and roles were known to the government at the time it received the seized emails from Yahoo!. *Id.* ¶¶ 30-31. The government has rejected repeated requests by the defense to identify the measures it took to identify privileged communications and those not related to the subjects set forth in the warrant. *Id.* ¶ 32 & Exs. 11-13. It is apparent, however, that even basic search terms to identify potentially privileged communications were not used. Over 5,600 emails in the database to which the prosecution team was given access contain the terms "privilege" or "privileged." Wade Decl. ¶ 28. Adding other common terms used to safeguard privileged materials, and properly factoring in the attachments to those communications, brings the total number to over 11,000 documents. *Id.* In the set of Yahoo! emails that were accessible to the prosecution team, more than 6,800 emails contain references to "attorney," "lawyer," or "counsel." *Id.* ¶ 29. Even the names of the lawyers and law firms *currently* representing Mr. Adams in his criminal case were apparently not used as search terms to identify potentially privileged materials. "Williams & Connolly" and the

names of Mr. Adams's counsel there appear in several documents in the folder to which the prosecution team was afforded access, even though the government was aware of Mr. Petrosinelli's representation of Mr. Adams no later than early March 2016. *Id.* ¶ 30. Sixty additional emails referring to Latham, Mr. Farrell, or Mr. Sikora—Mr. Adams's counsel in the parallel SEC investigation that only concluded in February 2017—are contained in the folder available to the prosecution team. *Id.* ¶ 31.

It was not until early September 2017 that the government agreed to suspend the prosecution team's access to the folder labelled "Adams_Yahoo_Unfiltered"—notwithstanding repeated prior requests from Mr. Adams's counsel that it do so. *Id.* ¶ 33 & Ex. 14.[3] By then, the prosecution team had had access to the folder for almost two years (approximately twenty months). *Id.* ¶ 34.

[3] Shortly before the government agreed to suspend the prosecution team's access to the folder, it also offered to establish a "taint team." Wade Decl. ¶ 35 & Exs. 11 & 14. Undersigned counsel have spoken to a representative of the proposed taint team, but the parties have not yet entered into any agreement regarding a taint team review, which may be inadequate under the circumstances existing in this case. Wade Decl. ¶ 36. In *United States v. Heppner*, Crim. No. 05-94 (JRT/FLN) (D. Minn.), where the government arranged for a "taint team" after a search, the court observed that it "share[d] the Magistrate Judge's skepticism" regarding the adequacy of a such a procedure, though finding it unnecessary to decide the issue. *See* Dkt. 79 at 4 n.1 (Nov. 23, 2005) (Doc. 79). Magistrate Judge Noel had rejected the use of a "taint team," describing it as "not unlike assigning the fox to guard the henhouse." Dkt. 71 at 11 n.3 (Oct. 13, 2005) (Doc. 71); *see also United States v. Neill*, 952 F. Supp. 834, 841 (D.D.C. 1997) ("Where the government chooses to take matters into its own hands rather than using the more traditional alternatives of submitting disputed documents under seal for *in camera* review by a neutral and detached magistrate or by court-appointed special masters, it bears the burden to rebut the presumption that tainted material was provided to the prosecution team." (citations omitted)). Undersigned counsel also advised the government of its intent to file this motion and sought to confer on the issues in dispute; the government

ARGUMENT

The government's handling of the Yahoo! emails violated the Fourth Amendment. The government led Magistrate Judge Rao to believe it would separate emails relevant to the subjects listed in the warrant application from other emails, but it then failed to take adequate steps to do so. It also withheld from Magistrate Judge Rao important information that would have shown that many of Mr. Adams's Yahoo! emails were likely privileged, and it later compounded that omission by failing to use even basic and obvious search terms to remove privileged and potentially privileged communications from the prosecution team's purview. The emails obtained from Mr. Adams's Yahoo! accounts and any evidence derived therefrom should be suppressed.

I. THE EMAILS WERE SEIZED UNDER AN OVERBROAD AND INVALID GENERAL WARRANT.

"[T]he Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 134 S. Ct. 2473, 2494 (2014). To prevent such abuses, the Warrant Clause of the Fourth Amendment commands that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing* the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "This particularity requirement 'ensures that the search will be carefully tailored to its

---

declined to confer and stated that the defense should file the motions that it deems appropriate.

justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.'" *United States v. Pennington*, 287 F.3d 739, 744 (8th Cir. 2002) (quoting *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)); *see also United States v. Apker*, 705 F.2d 293, 302 (8th Cir. 1983) ("[A] warrant must be as specific as possible."). "The uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5 (1984).

Both because the warrant in this case did not describe the things to be seized with particularity, and because the government did not take reasonable steps to do what the warrant contemplated or to protect the attorney-client and other privileges, the government violated the Fourth Amendment.

A. A Person's Email Account Is Protected by the Fourth Amendment.

In today's world, individuals often communicate by email. It is not surprising, therefore, that courts have overwhelmingly held that the protections of the Fourth Amendment extend to email. In the words of the Sixth Circuit, "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with . . . a commercial [internet service provider].'" *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently

> used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. ***By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.***

Id. at 284; *see also United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc) ("The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities.").

This Court likewise has found that the Fourth Amendment protects electronic communications, like email. As then-Chief Judge Davis observed,

> [I]t has been an established principle, at least since the Supreme Court's decision in *Katz v. United States*, that the Fourth Amendment protects individuals from intrusions upon their private electronic conversations.
>
> "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."

R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) (citation omitted) (quoting *Warshak*, 631 F.3d at 285–86). Other courts are in accord. *See United States v. Kitzhaber (In re Grand Jury Subpoena, JK-15-029)*, 828 F.3d 1083, 1090 (9th Cir. 2016) ("[E]mails are to be treated as closed, addressed packages for expectation-of-privacy purposes."); *Vista Mktg., LLC v. Burkett*, 812 F.3d 954, 969 (11th Cir. 2016); *United States v. Davis*, 785 F.3d 498, 528–29 (11th Cir.) (Rosenbaum, J., concurring) ("[O]ur expectation of privacy in our personal communications has not changed from what it was when we only wrote letters to what it is now that we . . . happen to use email to personally communicate."), *cert. denied*, 136 S. Ct. 479 (2015); *United States v. Zavala*, 541 F.3d 562, 577 (5th Cir. 2008) (defendant had

reasonable expectation of privacy with respect to "private information, including emails" stored on his cellular phone); *In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft Corp.*, 212 F. Supp. 3d 1023, 1034 (D. Kan. 2016) ("*Search of Microsoft*"); *United States v. Shah*, No. 5:13-CR-328-FL, 2015 WL 72118, at *11 (E.D.N.C. Jan. 6, 2015); *Murphy v. Spring*, 58 F. Supp. 3d 1241, 1268 n.19 (N.D. Okla. 2014); *In re Applics. for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, Nos. 13-MJ-8163-JPO, 2013 WL 4647554, at *3 (D. Kan. Aug. 27, 2013); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012); *United States v. Bode*, No. ELH-12-158, 2013 WL 4501303, at *15 (D. Md. Aug. 21, 2013); *see also United States v. Hamilton*, 701 F.3d 404, 408 (4th Cir. 2012) (recognizing, in marital privilege context, that "one may generally have a reasonable expectation of privacy in email").

B. The Warrant Improperly Authorized Seizure of All Data in the Three Email Accounts.

As it was treated by the government, the warrant served on Yahoo! was a textbook example of "the wide-ranging exploratory searches the Framers intended to prohibit." *Garrison*, 480 U.S. at 84. Absent exceptional circumstances, the Fourth Amendment prohibits examining an email or other social media account in its entirety merely because there is probable cause to believe a fraction of the data it contains may relate to alleged unlawful activity.[4]

[4] Federal Rule of Criminal Procedure 41(e)(2)(B), as amended in 2009, provides that a warrant may "authorize the seizure of electronic storage media or the seizure or copying

For example, in *United States v. Cioffi*, 668 F. Supp. 2d 385 (E.D.N.Y. 2009), the court granted a motion to suppress after the government seized from a defendant's email account all emails prior to the date that he had retained private counsel. *See id.* at 388–89. The court explained that "'[a] failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary.'" *Id.* at 391 (quoting *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992)). The warrant here was even broader than the one in *Cioffi* as the government posited no date restriction, an omission that was exacerbated when the government later failed to employ adequate filtering (including searches for the names of Mr. Adams's SEC and civil counsel) to avoided invading the attorney-client privilege.

In *United States v. Blake*, 868 F.3d 960 (11th Cir. 2017), the Eleventh Circuit recently criticized the government for serving warrants on Facebook that sought

---

of electronically stored information," and that "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." The advisory committee's note to the 2009 amendments explains that, because "[c]omputers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location[, t]his rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." The advisory committee's note expressly states, however, that "[t]he amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development."

"virtually every kind of data that could be found in a social media account." *Id.* at 974. Describing the breadth of the warrants as "unnecessar[y]," the court explained the tension with the Fourth Amendment:

> With respect to private instant messages, for example, the warrants could have limited the request to messages sent to or from persons suspected at that time of being prostitutes or customers. And the warrants should have requested data only from the period of time during which Moore was suspected of taking part in the prostitution conspiracy. Disclosures consistent with those limitations might then have provided probable cause for a broader, although still targeted, search of Moore's Facebook account. That procedure would have undermined any claim that the Facebook warrants were the internet-era version of a "general warrant."

Id. (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (plurality opinion)).

Consistent with this precedent, "authorizing [disclosure of] all email communications (including all content of the communications), and all records and other information regarding the [email] account is too broad and too general." *In re Applics. for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, Nos. 13-MJ-8163-JPO, 2013 WL 4647554, at *8 (D. Kan. Aug. 27, 2013) ("*Target Email Accounts*"); *accord, e.g.*, *United States v. Shah*, No. 5:13-CR-328-FL, 2015 WL 72118, at *14 (E.D.N.C. Jan. 6, 2015) (concluding that a warrant permitting seizure of all of the emails associated with a Gmail address "lack[ed] the particularity required by the Fourth Amendment"). The court deemed it "[m]ost troubling" that the warrants "fail to limit the universe of electronic communications and information to be turned over to the government to the specific crimes being investigated." *Target Email Accounts*, 2013 WL 4647554 at *8.

Similarly, in *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100 (N.D. Cal. 2014), the court denied on Fourth Amendment grounds an application for a warrant to seize, *inter alia*, "'[t]he contents of all e-mails associated with'" a Gmail account. *Id.* at 1102 n.2. The court was "unpersuaded that the particular seize first, search second proposed here is reasonable in the Fourth Amendment sense of the word." *Id.* at 1104. The overbreadth of the warrant was compounded by the government's failure to "ma[k]e any kind of commitment to return or destroy evidence that is not relevant to its investigation." *Id.*; *accord In re Search of Google Email Accounts Identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (denying an application that would have required Google to disclose all emails for six emails accounts). In this case, too, the government proposed to obtain all of the ESI associated with certain email addresses and only then to search within those files for documents relating to certain subjects; this approach, even if it had been followed, would have been unreasonable under the Fourth Amendment. Worse, the government did not follow this approach, but in fact turned over to the prosecution team a large volume of emails having nothing to do with the identified subjects.

Seizures of ESI were analyzed thoroughly in *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam), where the plurality warned that "[g]overnment intrusions into large private databases . . . have the potential to expose exceedingly sensitive information about countless individuals not implicated in any criminal activity, who might not even know that the information about them has been seized and thus can do nothing to protect their privacy." *Id.* at 1177. It

also stressed that "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id.* In a concurring opinion, five judges provided this guidance concerning searches of ESI:

> 2. Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. Pp. 1178-79 *supra*; *see* maj. op. at 1168-70, 1170-72. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
>
> . . . .
>
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents. Pp. 1178-79 *supra*; *see* maj. op. at 1170-72.
>
> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1180 (Kozinski, C.J., joined by Kleinfeld, W. Fletcher, Paez, and M. Smith, concurring).

Some decisions have sustained broad warrants for emails, but many either are distinguishable[5] or were issued before the Supreme Court's guidance in *Riley v.*

[5] In an early case, *United States v. Bach*, No. CRIM. 01-221 PAM/ESS, 2001 WL 1690055 (D. Minn. Dec. 14, 2001), *rev'd on other grounds*, 310 F.3d 1063 (8th Cir. 2002), where Judge Magnuson rejected a lack-of-particularity challenge to a warrant obtained by the Minnesota Internet Crimes Against Children Task Force that sought all emails to and from a specific email account at Yahoo, the account contained *only six emails*. *See* Brief of Appellant United States at 6, *United States v. Bach*, No. 02-1238 (8th Cir.) (explaining that police investigator received from Yahoo "all the emails

California, 134 S. Ct. 2473 (2014), regarding the need to guard against the threat to privacy posed by broad government access to ESI. *See id.* at 2491 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." (emphasis in original)).

The law is clear that emails and other ESI merit the same robust Fourth Amendment protections as tangible papers and at times may be even more vulnerable to unjustified government intrusion. As discussed above, procedures adopted by the government to address the practical challenges presented by ESI—such as the "seize first, search second" protocol employed in this case—do not obviate or supersede the paramount requirements of probable cause and particularity. Without a warrant that specifies limitations to at least time period, specific senders and recipients associated with the conduct under investigation, or other criteria designating the particular facts

---

preserved in defendant's" email account, "which amounted to five emails retrieved from defendant's 'In' box and one email from defendant's 'trash'").

Other readily distinguishable cases include *Search of Microsoft*, 212 F. Supp. 3d at 1037 (warrant for all email associated with certain accounts is proper if, *inter alia*, it "includes some limitations (such as a date range) to prevent the potential of a general search"), *United States v. Taylor*, 764 F. Supp. 2d 230, 232 (D. Me. 2011) (denying motion to suppress fruits of search of defendant's Microsoft hotmail account where government, upon seeing that there were emails to and from defendants' lawyers, successfully moved magistrate judge to approve "filter agent" procedure whereby an AUSA uninvolved with the prosecution would review the email materials and cull out any potentially privileged material before the investigation agent and the prosecution team received them"), and *United States v. Bowen*, 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010) (warrant for all email associated with certain email accounts was proper where "Defendants' alleged enterprise was primarily or solely criminal and Defendants used the target e-mail accounts as their primary e-mail accounts for conducting that business"), aff'd sub nom. *United States v. Ingram*, 490 F. App'x 363 (2d Cir. 2012).

being investigated, the search of a citizen's entire email account is unconstitutional. Yet, the government's warrant in this case did not contain *any* such boundaries, and it is clear from the state of the government's "filtered" and "unfiltered" databases that very few were introduced at any stage of its search of Mr. Adams's emails. The government's unwillingness to relinquish the numerous privileged and entirely irrelevant emails that (unsurprisingly) were swept up by its overbroad warrant compounds the intrusion into Mr. Adams's privacy, as other courts have recognized, and rebuts any suggestion by the government that it has been acting in good faith.

C. Courts Rigorously Apply Fourth Amendment Standards Where Confidential Attorney-Client Communications Are Implicated.

The government's conduct in this case is especially unacceptable because the government was on notice when it applied for the warrant of facts that made it likely that the warrant would cause the disclosure of a wide range of privileged communications.

The attorney-client privilege is "one of the oldest recognized privileges for confidential communications." *Swidler & Berlin v. United States*, 524 U.S. 399, 403 (1998). It reflects "the imperative need for confidence and trust" between lawyer and client, *Trammel v. United States*, 445 U.S. 40, 51 (1980), and "encourage[s] full and frank communication between attorneys and their clients and thereby promote[s] broader public interests in the observance of law and administration of justice," *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). The confidentiality of attorney-client communications is "not only an interest long recognized by society but also one traditionally deemed worthy of maximum legal protection." *Haines v. Liggett Grp. Inc.*,

975 F.2d 81, 90 (3d Cir. 1992). In the context of the government's criminal investigation, the SEC investigation, and the private civil suits, the attorney-client privilege was also inextricably tied to Mr. Adams's Fifth Amendment right to the advice and assistance of retained counsel.[6]

For this reason, courts apply greater scrutiny to searches likely to extend to confidential communications between attorney and client. *See, e.g.*, *United States v. Mittelman*, 999 F.2d 440, 445 (9th Cir. 1993) ("[S]pecial care should be taken when conducting a search of law offices . . . ."); *Nat'l City Trading Corp. v. United States*, 635 F.2d 1020, 1026 (2d Cir. 1980) ("[A] law office search should be executed with special care to avoid unnecessary intrusion on attorney-client communications.").

In this case, the government was well aware that the emails sent to or from edwardsadams@yahoo.com or jafman1@yahoo.com likely would include a large volume of privileged communications. It knew Mr. Adams was represented by counsel in the SEC investigation, which had been in progress since 2014. It knew he had been involved in related civil suits, and his representation by counsel in those suits was disclosed in publicly available court filings and dockets. It knew that for many years he had been

[6] *See, e.g.*, *Anderson v. Sheppard*, 856 F.2d 741, 747 (6th Cir. 1988) ("[T]he right of a civil litigant to be represented by retained counsel, if desired, is now clearly recognized."); *Mosley v. St. Louis Sw. Ry.*, 634 F.2d 942, 945 (5th Cir. Unit A Jan. 1981) ("The right to the advice and assistance of retained counsel in civil litigation is implicit in the concept of due process and extends to administrative, as well as courtroom, proceedings." (citation omitted)); *In re Taylor*, 567 F.2d 1183, 1186 n.1 (2d Cir. 1977) ("arbitrarily to forbid [a grand jury witness] from retaining a particular attorney . . . would deprive him of his constitutional right to due process of law").

General Counsel of Apollo Diamond. It knew that he had long been a partner at the law firm of Adams Monahan and that he had provided legal services for numerous clients of the firm.

For the government to take no steps either (i) to prevent or limit Yahoo!'s disclosure to it of attorney-client communications, or (ii) to set forth procedures in the warrant to safeguard the privacy such communications, renders its seizure of Mr. Adams's emails unconstitutional. Even when it is permissible for the government to seize material that it lacks probable cause to search (and it was not permissible to do so here), safeguards such as sorting or filtering procedures are required to keep searches in bounds:

> [E]ven if the Court were to allow a warrant with a broad authorization for the content of all email communications without a nexus to the specific crimes being investigated, the warrants would still not pass Constitutional muster. They fail to set out any limits on the government's review of the potentially large amount of electronic communications and information obtained from the electronic communications service providers. The warrants also do not identify any sorting or filtering procedures for electronic communications and information that are not relevant and do not fall within the scope of the government's probable cause statement, or that contain attorney-client privileged information.

Target Email Accounts, 2013 WL 4647554, at *8; *see also Comprehensive Drug Testing*, 621 F.3d at 1180 (Kozinski, C.J., concurring) ("Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the

investigators any information other than that which is the target of the warrant." (citations omitted)).

Nor can the government explain away its action by disclaiming any intention to use privileged communications. Apart from the lack of any reliable means of assuring that the government will not use knowledge gained from privileged material to shape the presentation of its case, the attorney-client privilege bars not only *use* of attorney-client communications against the client but also *disclosure* of attorney-client communications. *See, e.g., Chase Manhattan Bank, N.A. v. Turner & Newall, PLC*, 964 F.2d 159, 164 (2d Cir. 1992) ("The attorney-client privilege prohibits disclosure to adversaries as well as the use of confidential communications as evidence at trial."); *United States ex rel. Bagley v. TRW, Inc.*, 204 F.R.D. 170, 184 (C.D. Cal. 2001) ("The [attorney-client] privilege protects against both disclosure and use."). Indeed, protection against disclosure of privileged information is so strong that the Eighth Circuit held decades ago that although "[t]he writ of mandamus is not ordinarily available to a litigant to obtain appellate review of interlocutory discovery orders entered by a district court as litigation proceeds," such a writ is available "where a claim of attorney-client privilege has been raised in and rejected by a district court." *Diversified Indus., Inc. v. Meredith*, 572 F.2d 596, 599 (8th Cir. 1977).

II. THE WARRANT WAS EXECUTED IN AN UNREASONABLE MANNER.

Above and beyond the defects in the warrant itself, suppression is required because the government executed the warrant in a demonstrably unreasonable manner. "[T]he manner in which a warrant is executed is subject to later judicial review as to its

reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979).[7] In *United States v. Metter*, 860 F. Supp. 2d 205 (E.D.N.Y. 2012), the court granted a motion to suppress because the government, after seizing all information in personal email accounts and computers, unreasonably "delay[ed] [its] . . . review[] [of] the imaged evidence to determine whether the evidence that the government seized and imaged fell within the scope of the categories of information sought in the search warrants." *Id.* at 214–15; *see also id.* at 216 ("[T]he Court cannot, in the interest of justice and fairness, permit the government to ignore its obligations."). Similarly, the government's execution of the warrant in this case has been patently unreasonable.

Despite purporting to filter out potentially privileged emails and those unrelated to the subjects listed in the warrant, the government in fact gave its prosecution team access *for almost two years* to a folder containing hundreds of privileged communications as well as thousands of emails having nothing to do with the matters identified in the warrant. And it was not impractical for the government to locate and separate the privileged materials in that folder, as many are actually labelled "privileged" or were sent to or from attorneys for Mr. Adams whose involvement the government was aware of,

[7] *See also United States v. Medlin*, 842 F.2d 1194, 1199 (10th Cir. 1988) ("When law enforcement officers grossly exceed the scope of a search warrant in seizing property, the particularity requirement is undermined and a valid warrant is transformed into a general warrant thereby requiring suppression of all evidence seized under that warrant."); *United States v. Rettig*, 589 F.2d 418, 423 (9th Cir. 1978) (Kennedy, J.) ("As interpreted and executed by the agents, this warrant became an instrument for conducting a general search.").

and yet they wound up in the folder to which the prosecution team had access. *See* pp. 15-16, *supra*.

"The general touchstone of reasonableness which governs Fourth Amendment analysis, governs the method of execution of the warrant." *United States v. Ramirez*, 523 U.S. 65, 71 (1998) (citation omitted). It is patently unreasonable to execute a warrant in a manner that effectively converts it into one allowing examination of the entire contents of email accounts and needlessly leaves exposed material protected by one of the law's most important privileges.

III. THE GOOD FAITH EXCEPTION DOES NOT APPLY.

To the extent the government seeks refuge in the good faith exception recognized in *United States v. Leon*, 468 U.S. 897 (1984), it cannot carry its burden of demonstrating that the exception applies. In *Leon*, the Court limited the suppression remedy when "an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." 468 U.S. at 920. The government "'bears the burden of proving that its agents' reliance upon the warrant was objectively reasonable.'" *United States v. Cook*, 854 F.2d 371, 373 (10th Cir. 1988) (quoting *United States v. Michaelian*, 803 F.2d 1042, 1048 (9th Cir. 1986)); *accord United States v. Brunette*, 256 F.3d 14, 17 (1st Cir. 2001); *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992). *Leon*'s exception does not apply here for three reasons.

First, "[t]he good-faith exception does not apply . . . when the issuing judge is misled by information in the affidavit the affiant knows or should know is false . . . ." *United States v. Hessman*, 369 F.3d 1016, 1020 (8th Cir. 2004). "[O]nce a reviewing

court finds a search warrant affiant to be dishonest or reckless, suppression is appropriate under *Leon* regardless of whether or not the misrepresentation or omission would be material under *Franks*." *United States v. Boyce*, 601 F. Supp. 947, 955 (D. Minn. 1985); *see also, e.g.*, *United States v. Alexander*, 740 F. Supp. 437, 448 (N.D. Ohio 1990) ("Having deliberately presented [state court judge who signed warrant] with an inaccurate and incomplete picture, . . . the officers' present claim of good faith finds an unreceptive audience with this Court.").

Here, Inspector Kroells withheld from Magistrate Judge Rau information critically important to the likely impact of the seizure and thereby misled him. The Inspector did not inform Magistrate Judge Rau that Mr. Adams was represented by counsel in a parallel SEC investigation that had been underway since the preceding year, or that he had been represented by counsel in several related private civil suits, and that one of the email addresses at issue was his primary email address. To make matters worse, the Inspector listed several *non-legal* positions Mr. Adams had held with Apollo Gemstone and one *non-legal* position he held with Apollo Diamond, but failed to disclose the fact he had been General Counsel of Apollo Diamond for most of the period under investigation. And the Inspector stated that Magistrate Judge Mayeron had issued a warrant in late 2015, but failed to reveal that that warrant had contained an addendum setting forth procedures designed to limit access by the prosecution team to privileged communications. Withholding all of this information was not the action of a government official proceeding in good faith.

Second, any reliance by Inspector Kroells on Magistrate Judge Rau's approval of the warrant was unreasonable. *Leon* established that, for the good faith exception to apply, "the officer's reliance on the magistrate's probable-cause determination and on the technical sufficiency of the warrant he issues must be objectively reasonable, and it is clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Leon*, 468 U.S. at 922–23 (citation and footnotes omitted); *see United States v. Herron*, 215 F.3d 812, 815 (8th Cir. 2000). *Leon* further recognized that "a warrant may be so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923. The Supreme Court has since held that, "[g]iven that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid." *Groh v. Ramirez*, 540 U.S. 551, 563 (2004).

The Eighth Circuit "looks to the totality of the circumstances in assessing the objective reasonableness of an officer's execution of a warrant, '*including any information known to the officer but not presented to the issuing judge*.'" *United States v. Conant*, 799 F.3d 1195, 1202 (8th Cir. 2015), *cert. denied*, 136 S. Ct. 1214 (2016), *and cert. denied*, 136 S. Ct. 1233 (2016). In this case, Inspector Kroells knew or should have known important information that was not presented to Magistrate Judge Rau, including Mr. Adams's long-term tenure as General Counsel of Apollo Diamond, and his representation by counsel in the criminal investigation, the SEC investigation, and the four private civil suits. It was not objectively reasonable for her to seek a warrant that

plainly would cause Yahoo! to reveal numerous privileged communications, and yet to omit from the warrant any procedures (such as those contained in the first warrant) designed to limit access by the prosecution team.

Third, as a matter of law, the good faith exception cannot save the unreasonable ***execution*** of a warrant. The Supreme Court made clear in *Leon* that the good faith exception "assumes, of course, that the officers properly executed the warrant." *Leon*, 468 U.S. at 918 n.19. "[T]he good faith exception does not apply to the improper execution of a warrant." *United States v. Moland*, 996 F.2d 259, 261 (10th Cir. 1993); *See also Parks v. Commonwealth*, 192 S.W.3d 318, 335 (Ky. 2006) ("The 'good faith' exception will not save an improperly executed search warrant."); *State v. Cohen*, 957 P.2d 1014, 1017 (Ariz. Ct. App. 1998); *Sadie v. State*, 488 So. 2d 1368, 1378 (Ala. Crim. App. 1986); 1 Wayne R. LaFave, *Search and Seizure* § 1.3(f) at 89 (5th ed. 2012) ("Fourth Amendment violations relat[ed] to *execution* . . . are unaffected by *Leon* . . . ." (emphasis in original)). And as demonstrated in Part II, *supra*, the government's execution of the warrant has been unreasonable.

For each of these reasons, the government cannot carry its burden of demonstrating that the good faith exception applies.

IV. THE MOTION SHOULD BE GRANTED ON THE EXISTING RECORD, OR ALTERNATIVELY AN EVIDENTIARY HEARING SHOULD BE HELD.

The existing record demonstrates that the government violated the Fourth Amendment and the attorney-client privilege, and that therefore the data seized from Yahoo! and the evidence derived therefrom should be suppressed. *See Utah v. Strieff*,

136 S. Ct. 2056, 2061 (2016) ("Under the Court's precedents, the exclusionary rule encompasses both the 'primary evidence obtained as a direct result of an illegal search or seizure' and . . . 'evidence later discovered and found to be derivative of an illegality,' the so-called '"fruit of the poisonous tree."'" (quoting *Segura v. United States*, 468 U.S. 796, 804 (1984))); *United States v. Yousif*, 308 F.3d 820, 829 (8th Cir. 2002) ("Evidence that is the 'fruit' of an illegal search or seizure is not admissible, and '[t]he exclusionary prohibition extends as well to the indirect as the direct products of such invasions.'").

Alternatively, at a minimum, an evidentiary hearing should be held to develop a full record concerning the application for the warrant and the execution of the warrant. Such a hearing is necessary both because of the Fourth Amendment issues raised, *see, e.g.*, *United States v. Medlin*, 798 F.2d 407, 411 (10th Cir. 1986) ("[I]t is possible the police used this warrant as a pretext for a general search, which would taint the whole search. We therefore must remand this case to the district court for an evidentiary hearing to determine whether property was seized illegally, and, if so, whether the improper conduct was so flagrant that exclusion of *all* the seized evidence is warranted." (citation omitted)), and because of the issues relating to the attorney-client privilege, *see, e.g.*, *United States v. White*, 970 F.2d 328, 330 (7th Cir. 1992) (noting that court had previously remanded case "'for appropriate proceedings in the district court to determine . . . whether the government procured or was otherwise[] complicit in a violation of the attorney-client privilege'"); *United States v. Schwimmer*, 892 F.2d 237, 245 (2d Cir. 1989) (holding that "the district court should have conducted an evidentiary hearing to determine whether the government's case was in any respect derived from a violation of

the attorney-client privilege"); *United States v. Kleifgen*, 557 F.2d 1293, 1297 (9th Cir. 1977) (remanding for an evidentiary hearing concerning whether privileged communications were disclosed to the government); *United States v. Warshak*, No. 1:06-CR-00111, 2007 WL 3306603, at *1 (S.D. Ohio Nov. 5, 2007) (setting a "*Kastigar*-like" hearing to take testimony from government agents as to their handling of evidence because "[d]efendants had raised enough of a question about the amount of time [a government agent] possessed privileged data, as well as the government's methodology in screening data for privileged information, to merit a response"), *aff'd*, 631 F.3d 266 (6th Cir. 2010).[8] At such a hearing, the defense and the Court could question Inspector Kroells and other government agents involved in applying for and executing the warrant, to further explore the circumstances surrounding each of those actions.

[8] *See also United States v. DeLuca*, No. 6:11-cr-221-Orl-28KRS, 2014 WL 3341345, at *3 (M.D. Fla. July 8, 2014) (evidentiary hearings held "to determine what potentially privileged materials were accessed or used by the prosecution team"), *aff'd per curiam*, 663 F. App'x 875 (11th Cir. 2016), *cert denied*, 137 S. Ct. 1216 (2017); *United States v. Weissman*, No. S2 94 CR 760, 1996 WL 751386, at *1 (S.D.N.Y. Dec. 26, 1996) (evidentiary hearing held concerning alleged "improper receipt and use" by government "of material covered by Weissman's attorney-client privilege"); *United States v. Boffa*, 513 F. Supp. 517, 519 (D. Del. 1981) (evidentiary hearing held to evaluate defendants' claim that witness disclosed "confidential communications to the Government, in violation of their respective attorney-client privileges").

To facilitate ascertainment of the facts in cases involving seizures of materials likely to contain a large quantity of privileged attorney-client communications, some courts have appointed a special master. *See, e.g.*, *United States v. Stewart*, No. 02 CR. 396 JGK, 2002 WL 1300059, at *10 (S.D.N.Y. June 11, 2002); *United States v. Abbell*, 914 F. Supp. 519, 520–21 (S.D. Fla. 1995).

CONCLUSION

For the foregoing reasons, Mr. Adams respectfully requests that the Court enter an order suppressing the materials seized from Yahoo! and all evidence derived therefrom, and directing the government to destroy or return all of the information obtained from Mr. Adams's Yahoo! accounts. Alternatively, Mr. Adams asks that an evidentiary hearing be held to develop a full record concerning the application for the warrant and the execution of the warrant.

Dated: September 27, 2017

Respectfully submitted,

/s/ *James L. Volling*

James L. Volling (#113128)
Deborah A. Ellingboe (#26216X)
FAEGRE BAKER DANIELS LLP
2200 Wells Fargo Center
90 South Seventh Street
Minneapolis, MN 55420
Telephone: (612) 766-7000
Facsimile: (612) 766-1600
james.volling@faegrebd.com
debbie.ellingboe@faegrebd.com

Joseph G. Petrosinelli (DC Bar #434280)
Lance Wade (DC Bar #484845)
Sarah Lochner O'Connor (DC Bar #1012405)
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
Telephone: (202) 434-5000
jpetrosinelli@wc.com
lwade@wc.com
soconnor@wc.com

Attorneys for Defendant Edward S. Adams